UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/682,526	09/14/2001	Aviel D. Rubin	2000-0415	3764

26652 7590 07/13/2006

AT&T CORP.
ROOM 2A207
ONE AT&T WAY
BEDMINSTER, NJ 07921

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/682,526	RUBIN, AVIEL D.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Reopening of Prosecution - New Ground of Rejection After Appeal Brief

In view of the Appeal Brief filed on 4/17/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Claims 1-16 are presented for examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims1-3, 5-7, 9-11, and 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bailey, III, (U.S. Patent No. 5,659,614 and Bailey hereinafter), in view of Matyas et al., (U.S. Patent No. 7,010,689 and Matyas '689 hereinafter).

Regarding claims 1 and 9, Bailey discloses a method of backing up one or more files on a local device onto remote servers over a network comprising:

deriving a cryptographic key from a user-provided passphrase (i.e., Bailey's second encryption is performed by the transmission program based on internally generated keys)(col. 17, lines 1-15);

compressing one or more files and adding each of the files to a bundle (i.e., the compression program encrypts the number of characters, that is the data block, identified by the block length value using the encryption key returned from the data security card)(col. 18, lines 13-29), and encrypting the bundle using the first cryptographic key (i.e., a first level of encryption based on a client-

selected string of characters) prior to sending the bundle to the remote server (Col. 17, lines 38-67 and Col. 18, lines 1-45).

Bailey discloses generation of a second key (col. 17, lines 1-15), however; Bailey does not expressly disclose generating a second cryptographic key from a user-provided passphrase and generating an authentication code for the bundle using said second cryptographic key and adding the authentication code to the bundle.

However, Matyas '689 discloses generating a second cryptographic key from a user-provided passphrase (i.e., personal key k belonging to a user, derived from a user-supplied "passphrase/password"), and generating an authentication code (i.e., MAC, Message Authentication Code) for the bundle using said second cryptographic key and adding the authentication code to the bundle (col. 7, lines 25-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including generating a second cryptographic key from a user-provided passphrase and generating an authentication code for the bundle using said second cryptographic key and adding the authentication code to the bundle as disclosed by Matyas '689. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas to provide enhanced user authentication with the capability for greater granularity of access control (Matyas '689, col. 7, lines 52-65).

Regarding claims 5 and 13, Bailey discloses a method of restoring one or more files on remote servers to a local device over a network comprising:

deriving a first cryptographic key from a user-provided passphrase (i.e., Bailey's second encryption is performed by the transmission program based on internally generated keys)(col. 17, lines 1-15);

decrypting a bundle received from the remote server using the first cryptographic key (i.e., the first level of decryption based on a client-selected key)(col. 18, lines 45-53), and decompressing one or more files from the bundle (col. 18, lines 45-67 and col. 19, lines 1-5).

Bailey discloses generation of a second key (col. 17, lines 1-15), however; Bailey does not expressly disclose generating a second cryptographic key from a user-provided passphrase and generating an authentication code for the bundle using said second cryptographic key and adding the authentication code to the bundle.

However, Matyas '689 discloses generating a second cryptographic key from a user-provided passphrase (i.e., personal key k belonging to a user, derived from a user-supplied "passphrase/password")(col. 11, lines 17-29); and

checking an authentication code (i.e., MAC, Message Authentication Code) for the bundle using said second cryptographic key and adding the authentication code to the bundle (col. 12, lines 15-67 and col. 13, lines 1-8).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for

including generating a second cryptographic key from a user-provided passphrase and generating an authentication code for the bundle using said second cryptographic key and adding the authentication code to the bundle as disclosed by Matyas '689. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas '689 to provide enhanced user authentication with the capability for greater granularity of access control (Matyas '689, col. 7, lines 52-65).

Regarding claims 2, 6, 10, and 14, Bailey discloses wherein a data block comprising different amount of data is encrypted using a client-selected symmetric key (col. 17, lines 1-15).

Matyas '689 discloses encrypting the file or pieces of the file with k.sub.e using a symmetric encryption algorithm (col. 9, lines 55-67 and col. 10, lines 1-32).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including wherein the bundle is encrypted using a strong block cipher as disclosed by Matyas '689. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas '689 provide enhanced user authentication with the capability for greater granularity of access control (Matyas '689, col. 7, lines 52-65).

Regarding claims 3, 7, 11, and 15, Bailey does not expressly disclose wherein the authentication code is an HMAC.

However, Matyas '689 discloses wherein the authentication code is an HMAC (col. 9, lines 20-67 and col. 10, lines1-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including generating a second cryptographic key from a user-provided passphrase and generating an authentication code (i.e., HMAC) for the bundle using said second cryptographic key and adding the authentication code to the bundle as disclosed by Matyas '689. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas '689 to provide enhanced user authentication with the capability for greater granularity of access control (Matyas '689, col. 7, lines 52-65).

Claims 4, 8, 12, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bailey, III, (U.S. Patent No. 5,659,614 and Bailey hereinafter) and Matyas et al., (U.S. Patent No. 7,010,689 and Matyas '689 hereinafter), in view of Matyas et al., (U.S. Patent No. 5,201,000 and Matyas '000 hereinafter).

Regarding claims 4, 8, 12, and 16, Bailey and Matyas '689 are both silent about the length of their encryption key.

However, Matyas '000 discloses wherein the cryptographic keys contain at least 128 bits (i.e., DEA keys are 64 or 128 bits)(col. 13, lines 63-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Bailey and Matyas '689 by including DEA keys which are specifically 128 bits long as disclosed by Matyas '000. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas '000 to facilitate a secure encryption channel between sending and receiving devices (col. 3, lines 25-55).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cane et al., (U.S. Patent No. 5,940,507),

Elander et al., (U.S. Patent No. 5,323,464),

Halter et al., (U.S. Patent No. 5,319,705), and

Matyas et al., (U.S. Patent No. 5,142,578).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax

phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.

Patent Examiner
Group 2131
July 3, 2006

Christopher Revak
Primary Examiner
AU 2131
7/6/06